Federal Public Key Infrastructure Policy Authority

Charter, Bylaws, and Operational Procedures

Version 1.0

January __, 2015

1.0 BACKGROUND AND PURPOSE

1.1 BACKGROUND

The Federal Public Key Infrastructure (FPKI) is supported by the FPKI Policy Authority (PA) and the FPKI Management Authority (MA). GSA's Office of Government-wide Policy currently provides secretariat and subject matter expertise support for the PA, while the MA is run by GSA's Federal Acquisition Services and provides operational support and maintains the FPKI Trust Infrastructure in accordance with the FPKI Certificate Policies and Certification Practice Statements approved by the PA.

The PA was codified by the Federal Chief Information Officers Council in 2000 to serve as the Federal Bridge governing body. The PA includes entities operating enterprise Public Key Infrastructures (PKIs) cross-certified with the Federal Bridge Certification Authority (FBCA) or the Federal Common Policy Certification Authority (FCPCA) or who have acquired PKI services under the Shared Service Provider (SSP) Program, and who have demonstrated their interest in participating in the work of the PA.

1.2 FPKI VALUE STATEMENT

The FPKI provides numerous services that directly benefit federal agency business needs and objectives,[1] including fundamental high-assurance trust services for a wide variety of customers. It contains the Federal Government's PKI trust anchor and facilitates trust of Personal Identity Verification (PIV), PIV-Interoperable (PIV-I), and other government and non-government credentials. As a result, the FPKI is essential for federal agency physical and logical access solutions and is of great importance to citizens, businesses, and organizations that need access to federal agency services and facilities.

The FPKI is needed for federal agencies to comply with HSPD-12 and Executive Office of the President (EOP) Office of Management and Budget (OMB) Memorandum M-11-11, accept PIV-I Cards, and accept third-party credentials as discussed in National Strategy for Trusted Identities in Cyberspace (NSTIC) and directed by OMB VanRoekel Memorandum dated October 6, 2011. In addition, the FPKI is a key enabler of electronic business process flows within and between organizations and supports other Federal Identity, Credential, and Access Management (FICAM) initiatives, such as Backend Attribute Exchange.

1.3 AUTHORITY

The PA operates under authority of the Federal CIO Council through the Information Security and Identity Management Committee (ISIMC) and the Identity, Credential, and Access Management Subcommittee (ICAMSC).

[1] *See The Realized Value of the FPKI for federal agency use cases and benefits attained.*

The Federal CIO Council or its assignee issues and updates this charter of operations; appoints the PA leadership; and oversees FPKI responsibilities, work plans, and priorities.

1.4 Purpose

The PA sets policy governing the FPKI Trust Infrastructure; approves applicants for cross certification with the FBCA, including PIV-I issuers, and provides oversight for the Certified PKI SSP Program. The PA serves the interest of U.S. Government organizations as relying parties and promotes interoperability between federal and non-federal entities.

2.0 RESPONSIBILITIES OF THE FEDERAL PKI POLICY AUTHORITY

The PA has the following responsibilities:

2.1 CP/CPS Change And Approval

- Approving the FBCA Certificate Policy (CP), including revisions
- Approving the FCPCA CP, including its revisions
- Approving the EGCA CP, including its revisions
- Approving the FPKI Trust Infrastructure Certification Practices Statements (CPS)

2.2 Approval of Entity Cross-Certification

- Establishing and administering the *Criteria and Methodology for Cross-Certification with the U.S. FBCA* [CRITS&METHODS] for entities wishing to cross-certify with the FPKI, including the approval of all entity cross-certifications and execution of resultant Memoranda of Agreement (MOA)
- Maintaining the FPKI Certification Applicant Requirements (mapping criteria for the FBCA) and the Common Policy CPS Evaluation Matrix to ensure continued accuracy and relevance in relation to the supported policies

2.3 Maintain Compliance

- Ensuring cross-certified entities remain compatible with the FBCA CP (or the FCPCA CP for Federal Legacy CAs) by implementing the enforcement mechanisms in the [CRITS&METHODS]
- Ensuring that Certified SSPs comply with the ongoing requirements for participation including requirements for maintaining compliance as described in the SSP Roadmap

2.4 Agreement With FPKI Management Authority

Establishing and maintaining a relationship with the FPKI Management Authority (MA), to include:

- Directing the MA concerning the issuance and revocation of cross-certificates

- Ensuring MA continued adherence to the FPKI CPs
- Providing documentation to the MA for archives

2.5 Interoperability Practices

Coordinating legal, policy, technical, and business practices and issues related to FPKI Trust Infrastructure interoperability.

3.0 MEMBERSHIP AND ORGANIZATION

3.1 Membership

Membership in the PA is open to federal agencies that have cross-certified with the FBCA or FCPCA, federal agencies using PKI certificate services acquired through an approved SSP, cross-certified non-federal government PKIs and PKI bridges that have a fully-executed MOA or contract with the federal government, and ex officio members as designated below.

Each federal agency representative shall be appointed by the CIO of their agency.

Membership terminates if and when the Entity (Shared Service Providers, Bridges Cross Certified with the FPKI) ceases to operate its cross-certified CA or PKI SSP model or chooses not to participate in the PA.

Voting membership for the PA is reserved for federal entities. All other members are non-voting.

Voting Membership

Voting membership for the FPKIPA is reserved for federal entities:

FPKI Cross Certified Federal Entities

All federal agencies, independent commissions, and organizations that operate self-signed PKIs that have successfully completed the process of cross-certifying with the FPKI Trust Infrastructure in accordance with [CRITS&METHODS] are eligible to be voting members of the FPKIPA.

Agencies Acquiring Certificate Services through a Certified PKI SSP

Federal agencies acquiring PKI certificate services from a Certified PKI SSP are eligible to be voting members of the FPKIPA.

General Criteria for All Voting Members

Voting membership in the FPKIPA for eligible federal entities is granted and maintained under the following circumstances:

a) The agency expresses a desire to become a new voting member of the FPKIPA by submitting an application for membership, and

b) The agency makes the requisite commitment of time and resources as evidenced by regular FPKIPA and working group participation.

Suspension of Voting Privileges

Agencies may have their voting privileges temporarily suspended by a vote of the FPKIPA if the requisite commitment of time and resources, as evidenced by regular FPKIPA and working group participation, is not met.

An agency may return to full voting membership when the circumstances that led to suspension have been resolved and the reinstatement has been approved by a FPKIPA vote.

Ex Officio Membership

The following have ex officio membership:

(1) OMB and designees from the Federal CIO Council
(2) Co-chairs of the ICAMSC
(3) Program Managers of MA and PA
(4) Other representatives as appointed by the Co-Chairs of the PA.

Ex officio membership does not confer voting privileges, but are welcome to participate on working groups and subcommittees at their discretion.

3.2 COMMITTEES/WORKING GROUPS

The PA may create, participate in, or dissolve working groups to support its activities. Each group established under the PA shall have a Chair or Co-Chairs appointed by the PA Co-Chairs and announced to the PA membership. A group Chair must be a federal employee; however, a non-federal employee supporting a voting member organization may be appointed as a Co-Chair.

The current existing working groups of the PA are:

FPKI Certificate Policy Working Group (CPWG)

Reviews and maintains Applications for Cross-Certification, CPs, CP Change Proposals, and auditor reports of entities that apply for or seek to maintain cross-certification with the applicable FPKI Trust Infrastructure CA at a specific level of assurance, and recommends to the PA the acceptance or rejection of these entity applications, CPs, and audit reports.

The CPWG also maintains FPKI CPs, administrative and guidance documents (e.g. Criteria and Methodology for Cross-Certification with the U.S. Federal Bridge Certification Authority (FBCA), FPKI Certification Applicant Requirements) and recommends changes to those documents to the PA.

PKI Shared Service Provider Working Group (SSPWG)

Oversees the processes involved in the Certified PKI Shared Service Provider (SSP) Program. These processes are documented in the SSP Roadmap document. SSPWG Membership is limited to federal employees and direct-support contractors on behalf of their agencies, as well as approved PKI SSP vendors.

FPKI Technical Working Group (TWG)

Reviews and provides advice about technical issues related to the FPKI at the request of the PA, CPWG, or Federal PKI MA.

4.0 LEADERSHIP

PA CO-CHAIRS

There shall be two co-chairs of the PA. Both will be appointed by the Federal CIO Council or its assignee. The Federal CIO Council will also determine which Co-Chair shall be the signatory executor of all PA documents, such as CPs, MOAs, LOAs, etc.

The Co-Chairs shall, at a minimum, be responsible for:

- Chairing PA meetings
- Serving as liaison in keeping the Federal CIO Council or its assignees informed of PA activity
- Ensuring the PA adheres to the Federal CIO Council-approved responsibilities, work plans, and priorities and coordinating all FPKI activities, such as promoting the use of PKI to serve the interest of the Federal Government and other organizations (i.e. commercial, international, etc.)
- Determination of remedies/actions to be taken for noncompliance and/or unacceptable risk, or to restore Federal Bridge Certification Authority (FBCA) and Federal Common Policy CA (FCPCA) interoperability following cross-certificate revocation.
- Re-issuance of a Member’s cross-certification under extraordinary circumstances.
- Sending compliance audit letter notifications

5.0 OPERATIONS

5.1 MEETINGS

PA meetings shall be held on a regular schedule as determined by the PA Co-Chairs. The meeting time and location may be modified as needed.

The quorum necessary for the PA to transact official business shall be two-thirds (2/3) of the voting membership. A transmitted proxy to an attending member shall also count toward a quorum.

5.2 VOTING

The Co-Chairs shall decide when a vote is to be taken, either during a meeting or outside a meeting by email. The Co-Chairs will first ask for a general vote of all members in favor and all members opposed. Only for more controversial or split votes will a roll call vote be used. A Voting Member may provide a proxy to another Voting Member during a single meeting.

Voting Members may request a vote without a meeting or the Co-Chairs call for online discussion and/or voting, (i.e., “Call for an Electronic or Email Vote”). Voting Members shall have at least five business days to vote. The Co-Chairs may request a shorter timeframe when the need is urgent.

Electronic Voting

When a member votes by electronic means (e.g., email), the electronic vote shall be signed to indicate the member’s intent to vote and confirm that member’s identity. The electronic vote should contain a valid PKI digital signature. Failure to use the above methods shall cause the electronic vote to be considered invalid and not counted in the tally. The Co-Chairs may waive the requirement to use a valid PKI digital signature for a voting member in a case-by-case basis.